WG#15: Securing Mobile Code

Report Summary

- **Problem Description / Technical Scope**
  - Mobile Code Security / Distributed Computing
- **Relevant Disciplines / Technologies**
  - Security, Programming Languages, High Assurance Systems, Formal Methods, Computing Environments, Executable Content (e.g., Java)
- **Major Technical Challenges**
  - Protecting Hosts, Mobile Program, static resources, the Infrastructure. Defining interoperable security policies and specifications.

Addressing the Challenges

- Challenges
  - Protecting hosts from agents
  - Protecting agents from hosts and other agents
- Novel Approaches
  - Defining interoperable security policies
  - A continuum of mechanisms (e.g., authentication, code validation/verification, and controlled execution environments.

Projected Outcome

- Coordinated use of Trusted, authenticated mobile applications
  - information gathering/filtering, shopping, mobile cash
  - success likely with interoperable security policies
- Safe use of Untrusted, anonymous Agents
  - information gathering/filtering, sporadic connectivity
  - success likely with controlled execution environments

Investment Strategy

- **DARPA, Industry Support**
  - **Why DARPA? Industry track record focuses on functionality, not security**
  - **What other collaborations? University/industry: numerous mobile code systems currently in development**
- **What if we did not do this?**
  – increasingly insecure global computing environment
- **Optimal Scale of Efforts**
  - **small-scale for policy environment**
  - **large-scale active networks**

Other Issues Addressed

- Host vs agent perspectives
- Assurance
- Fault tolerance
- Auditing
- Lightweight security mechanisms
- Formal methods/languages
- Formal model of mobile computing